

a location for transmission of the secure container, and
controls associated with use or transmission of the secure
container;

means for transmitting secure containers to locations designated by the
secure container information, the means for transmitting capable of
operating at least in part under control of controls associated with the
secure containers; and

means for associating routing information with secure containers, the
routing information including information indicating that the secure
containers passed through the first checkpoint.

22. A system as in Claim 21, further including:

a second checkpoint adapted for communicating digital information to and
from the first checkpoint, the second checkpoint including:

a switch including means for receipt and routing of digital information;
means for detecting the presence of secure containers;

means for determining information regarding secure containers, the
information including:

a location for transmission of the secure container, and
controls associated with use or transmission of the secure
container;

means for transmitting secure containers to locations designated by the
secure container information, the means for transmitting capable of
operating at least in part under control of controls associated with the
secure containers; and

A18

means for associating routing information with secure containers, the
routing information including information indicating that the secure
containers passed through the second checkpoint.

23. A system as in Claim 22, further including:

means at the first and second checkpoints for generating digital
certificates, the digital certificates including information identifying the
checkpoint which generated the certificate and including information as
to the security level of the checkpoint which generated the certificate.

24. A system as in Claim 23, in which:

the first and second checkpoints are designated as having a first
security level, and the system further including:

a third and fourth checkpoint, each including:

a switch including means for receipt and routing of digital information;
means for detecting the presence of secure containers;

means for determining information regarding secure containers, the
information including:

A¹³
a location for transmission of the secure container;
controls associated with use or transmission of the secure
container;

means for transmitting secure containers to locations designated by the
secure container information, the means for transmitting capable of
operating at least in part under control of controls associated with the
secure containers; and

means for associating routing information with secure containers, the
routing information including information indicating that the secure
containers passed through the checkpoint.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-8600

25. A system as in Claim 24, in which:

the third and fourth checkpoints are designated as having a second security level, which is relatively more secure than the first security level.

26. A system as in Claim 25, further including:

A¹⁰
a secure container including governed content and at least one control specifying that the secure container must be routed through one or more checkpoints with the second security level.

27. A method of routing a secure container, the secure container including governed content and having associated a rule set at least in part governing access to or other use of the governed content, the method including:

sending the secure container from a sender to a first secure checkpoint;

at the first checkpoint, ascertaining routing information from the rule set and determining, based on the routing information, that the first secure checkpoint is authorized to receive and transmit the secure container;

at the first secure checkpoint, determining, based on the routing information, that the secure container is to be transmitted to a first recipient;

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

at the first secure checkpoint, associating first checkpoint information with the secure container, the first checkpoint information indicating that the secure container was received by and transmitted by the first secure checkpoint;

transmitting the secure container, including the associated first checkpoint information, to a first recipient, the transmission being governed, at least in part, by the rule set;

A¹ at the first recipient, ascertaining routing information from the rule set and determining, based on the routing information, that the first recipient is authorized to receive the secure container;

at the first recipient, determining, from the rule set, that the rule set specified a required path for transmission of the secure container from the sender to the first recipient;

at the first recipient, comparing the first checkpoint information with the specified required path; and

based on a match between the first checkpoint information and the specified required path, the first recipient undertaking an action involving the secure container.

28. A method as in Claim 27, further including:

the first checkpoint transmitting audit trail information to the sender, the audit trail information indicating that the secure container was received by the first checkpoint and transmitted by the secure checkpoint to the first recipient.

29. A method as in Claim 28, further including:

the first recipient transmitting audit trail information to the sender, the audit trail information indicating that the secure container was received by the first recipient.

30. A method as in Claim 29, in which:

the first recipient constitutes a second secure checkpoint, and the action undertaken by the first recipient includes:

ascertaining routing information from the rule set and determining, based on the routing information, that the first recipient is authorized to receive and transmit the secure container;

determining, based on the routing information, that the secure container is to be transmitted to a second recipient;

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

associating second checkpoint information with the secure container, the second checkpoint information indicating that the secure container was received by and transmitted by the first recipient; and

transmitting the secure container, including the associated second checkpoint information, to a second recipient, the transmission being governed, at least in part, by the rule set; and

A¹

at the second recipient, ascertaining routing information from the rule set and determining, based on the routing information, that the second recipient is authorized to receive the secure container;

at the second recipient, determining, from the rule set, that the rule set specified a required path for transmission of the secure container from the sender to the first recipient;

at the second recipient, comparing the first checkpoint information and the second checkpoint information with the specified required path; and

based on a match between the first checkpoint information, the second checkpoint information and the specified required path, the second recipient undertaking an action involving the secure container.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

31. A method as in Claim 30, in which the second recipient action includes:

opening at least a portion of the secure container; and
transmitting audit trail information to the sender, the audit trail
information indicating that the secure container was received by the
second recipient.

32. A method including:

generating a secure container including governed contents;

A¹ associating a rule set with the secure container, the rule set including at
least one rule designed to at least in part govern access to or other use
of the governed contents;

associating a first digital certificate with the secure container, the first
digital certificate including a digital signature;

transmitting the secure container, including the associated rule set and
first digital certificate, from a first site to a first secure checkpoint;

at the first secure checkpoint, reading routing information, the routing
information indicating an intended recipient of the secure container;

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

at the first secure checkpoint, associating a second digital certificate with the secure container, the second digital certificate including a digital signature and information evidencing the receipt of the secure container at the first secure checkpoint;

transmitting the secure container, including the associated rule set and first and second digital certificates to the intended recipient;

A¹²
at the intended recipient, reading information from the first certificate and the second certificate, the information relating to the actual route taken by the secure container between the first site and the intended recipient; and

based on the actual route information, taking an action.

33. A method as in Claim 32, in which the action includes comparing the actual route information to a specified or required route.

34. A method as in Claim 33, further including:

if the comparison indicates that the actual route information is consistent with the specified or required route, accessing at least a portion of the secure container contents; and

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

if the comparison indicates that the actual route information is not consistent with the specified or required route, sending an indication of the inconsistency to the first site.

35. A method as in Claim 32, further including:

choosing the first secure checkpoint from at least two secure checkpoints, the choice being governed at least in part by the rule set, the choice being made prior to the transmission of the secure container to the first secure checkpoint.

AI

36. A method as in Claim 35, in which:

the choice of the first secure checkpoint is based on an affiliation between that checkpoint and other checkpoints.

37. A method including:

generating a rule set specifying a level of insurance dependent, at least in part, on use of a specified secure checkpoint route;

associating the rule set with a secure container;

transmitting the secure container from a sending site to a receiving site, the transmission proceeding through a first secure checkpoint;

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

at the first secure checkpoint, associating first information with the secure container, the first information specifying that the secure container was received by and transmitted from the first secure checkpoint;

receiving the secure container at the receiving site; and

at the receiving site, using the first information to determine if the route followed by the secure container from the sending site to the receiving site was consistent with the specified secure checkpoint route.

38. A method as in Claim 37, further including:

receiving the secure container at a second secure checkpoint, at the second secure checkpoint, associating second information with the secure container, the second information specifying that the secure container was received by and transmitted from the second secure checkpoint; and

at the receiving site, using the second information along with the first information in determining if the route followed by the secure container from the sending site to the receiving site was consistent with the specified secure checkpoint route.

39. A method as in Claim 38, in which:

the step of transmitting the secure container from the sending site to the receiving site includes choosing the first secure checkpoint and the second secure checkpoint from among a plurality of checkpoints available for the transmission, the choice being governed, at least in part, by the rule set.

40. A method as in Claim 37, further including:

A/b
following the determination by the receiving site as to whether the route followed was consistent with the specified secure checkpoint route, sending a communication relating to the results of that determination to the sending site.

41. A method as in Claim 37, further including:

following the determination by the receiving site as to whether the route followed was consistent with the specified secure checkpoint route,

if the determination indicates that the specified route was followed, accessing at least a portion of the secure container contents; and

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

if the determination indicates that the specified route was not followed, blocking access to the secure container contents and sending a communication to the sending site.

42. A secure checkpoint including:

means for receiving and transmitting secure containers, the secure containers including content and having associated a rule set designed to at least in part govern use of the content;

means for opening secure containers so as to obtain access to at least a portion of the contained content;

means for using the associated rule set to identify a required route for transmission of the associated secure container;

means for determining whether a secure container has followed the required route; and

means for associating a certificate with a secure container, the certificate including information relating to whether the secure container has followed the required route.

A!

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

43. A secure checkpoint as in Claim 42, further including:
means for reviewing certificates associated with secure containers,
including means for determining whether certificates have expired.
44. A secure checkpoint as in Claim 43, further including:
a memory storing a certificate revocation list and means for comparing
certificates to the revocation list.
45. A secure checkpoint as in Claim 44, further including:
a directory service including information relating to electronic addresses
for potential recipients of secure containers.
46. A secure checkpoint as in Claim 45, in which the directory service includes
public keys of potential recipients of secure containers.
47. A network including:
a first network node including:
a secure checkpoint including means for receiving secure
containers, means for reading information associated with secure
containers to determine secure container routing information and
means for transmitting secure containers in accordance with the routing
information;

a certification authority including means for issuing digital certificates attesting to the validity of information, and means for associating certificates with secure containers received by the secure checkpoint, the associated certificates including information indicating that the secure container was received by the secure checkpoint; and

A 10
a directory service including a memory storing address information relating to potential recipients of secure containers and means for associating recipient address information with secure containers, the recipient address information associating means being capable of operating at least in part under control of a rule set associated with the secure container.

48. A network as in Claim 47, further including:

a second network node including:

a secure checkpoint including means for receiving secure containers, means for reading information associated with secure containers to determine secure container routing information, and means for transmitting secure containers in accordance with the routing information.

49. A network as in Claim 48, further including:

a third network node including:

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

a secure checkpoint including means for receiving secure containers, means for reading information associated with secure containers to determine secure container routing information, and means for transmitting secure containers in accordance with the routing information; and

a fourth network node including:

A 1
a secure checkpoint including means for receiving secure containers, means for reading information associated with secure containers to determine secure container routing information, and means for transmitting secure containers in accordance with the routing information;

wherein the first network node and the second network node include a first identifier identifying them as belonging to a first web of nodes and the third network node and the fourth network node include a second identifier identifying them as belonging to a second web of nodes.

50. A network as in Claim 47, in which:

the first network node further includes means for determining whether secure containers have been received from a source consistent with the routing information, and means for transmitting a report if the secure container was not received from such a source.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

51. A network as in Claim 47, in which:

the first network node further includes memory means for archiving
information relating to secure containers received by the first network
node secure checkpoint.

52. A first digital certificate including:

information certifying a fact, digital file, or process;

issuer identification information including information relating to the
identity of an issuer of the first digital certificate; and

liability protection information including information relating to the
amount of liability the issuer is willing to accept in the event the
authentication information is inaccurate.

53. A first digital certificate as in Claim 52, further including:

authentication information encrypted with the private key of the issuer.

54. A first digital certificate as in Claim 53, further including:

location information relating to a location from which the public key of
the issuer may be obtained.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

55. A first digital certificate as in Claim 52, further including:
information relating to an expiration date for the first digital certificate.
56. A first digital certificate as in Claim 52, further including:
information at least in part identifying a second digital certificate which
certifies information upon which the first digital certificate is based at
least in part.
57. A digital certifying authority including the following:
means for the creation of digital certificates, including:
A means for signing the digital certificates;
a secure communications facility;
means for evaluating digital certificates received from third parties through
the secure communications facility, including means for checking the
validity and authenticity of the digital certificates and
means for reporting results;
the means for evaluating digital certificates being capable of operating
at least in part under the control of rules received in a secure container,

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

the secure container being received through the secure
communications facility;

an encryption/decryption processor;

a billing system, including means for billing third parties for the creation of and
evaluation of digital certificates;

AI
 a key generator;

an electronic archive storing keys and digital certificates; and

a query mechanism designed to retrieve keys and digital certificates from the
electronic archive.

58. A digital certifying authority as in Claim 57, further including a usage
clearinghouse designed to at least part clear electronic transactions.

59. A digital certifying authority as in Claim 57, in which the electronic archive
further stores a list of revoked digital certificates.

60. A digital certifying authority as in Claim 57, in which the electronic archive
further stores information relating to the amount of liability at least one certificate

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

issuer is willing to accept in the event a digital certificate is determined to be false or to contain erroneous information.

61. A digital certifying authority as in Claim 57, further including means for issuing multiple digital certificates for the same individual or entity, the multiple digital certificates each including a common identifier.

62. A virtual distribution environment administration node including:

means for configuring protected processing environments at user sites;

ANI certification means for issuing digital certificates an aspect of protected processing environments configured at user sites; and

memory means for securely storing issued certificates and keys associated with configured protected processing environments.

63. A virtual distribution environment administration node as in Claim 62, in which:

the certification means includes means for issuing digital certificates certifying information relating to individuals, including age.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-649-6600

64. A virtual distribution environment administration node as in Claim 62, in which:
the certification means includes means for issuing digital certificates
certifying information relating to individual membership in a group or
class.
65. A virtual distribution environment administration node as in Claim 62, in which:
the certified aspect of configured protected processing environments
includes certification of a level of security present at the certified
protected processing environment, where at least two security levels are
possible.
66. A virtual distribution environment administration node as in Claim 62, in which:
the certification means includes means for issuing digital certificates
certifying information relating to operation of a clearinghouse.
67. A method including the following steps:
generating a first virtual entity certificate an identifier related to a first
virtual entity, and a digital signature of a first member of the first virtual
entity;

embedding the first virtual entity certificate into a secure container having
a first associated rule set at least in part governing use of the first virtual
entity certificate, the first associated rule set including a rule governing

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

the circumstances under which the first member may perform an action on behalf of the first virtual entity;

the first member extracting the first virtual entity certificate from the secure container, the extraction being governed at least in part by the first associated rule set; and

the first member performing an action on behalf of the first virtual entity, the action being governed at least in part by the first associated rule set, the first member's authority to perform the action being certified by the first virtual entity certificate.

A1

68. A method as in Claim 67, further including:

generating a second virtual entity certificate including an identifier related to a first virtual entity, and a digital signature of a second member of the first virtual entity; and

embedding the second virtual entity certificate into the secure container, the secure container having a second associated rule set at least in part governing use of the second virtual entity certificate, the second associated rule set including a rule governing the circumstances under which the second member may perform an action on behalf of the first virtual entity.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600

69. A method as in Claim 67, in which:

the first member's action includes generating or altering a digital certificate, the generation or alteration being accomplished by the first member as a representative of the virtual entity.

70. A method as in Claim 68, in which:

the step of embedding the first virtual entity certificate into the secure container occurs in a protected processing environment located in a computer associated with the first member.

71. A method as in Claim 70, in which:

the step of embedding the second virtual entity certificate into the secure container occurs in a protected processing environment located in a computer associated with the second member, and

the secure container, or a copy of the secure container, is then directly or indirectly transmitted to the protected processing environment associated with the first member.

A 1

72. A system for supporting a virtual entity comprising:

plural distributed, trusted electronic commerce nodes for use by plural parties, one or more said trusted electronic commerce nodes securely creating one or more digital credentials representing a virtual entity comprising a cooperative participation among plural parties and/or nodes for one or more commercial purposes;

A a digital credentialing arrangement that issues digital credentials to said plural parties and/or nodes to at least in part represent the identity of said parties and/or nodes; and

a secure communications arrangement that securely communicates among said plural parties and/or nodes, digital information related to at least in part the identity of said parties and/or nodes,

wherein said system employs at least one of said one or more credentials representing said virtual entity to, at least in part, enable said virtual entity to at least in part participate in at least one commercial process.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT
& DUNNER, L.L.P.
STANFORD RESEARCH PARK
700 HANSEN WAY
PALO ALTO, CALIF. 94304
650-849-6600